PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Patent Office
Canberra

I, LEANNE MYNOTT, MANAGER EXAMINATION SUPPORT AND SALES hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. 2002952669 for a patent by SECURENCY PTY LIMITED as filed on 14 November 2002.

WITNESS my hand this
Twenty-fourth day of November 2003

LEANNE MYNOTT
MANAGER EXAMINATION SUPPORT AND SALES

AUSTRALIA

Patents Act 1990

PROVISIONAL SPECIFICATION

Invention Title: **Tamper evident security document**

The invention is described in the following statement:

TAMPER EVIDENT SECURITY DOCUMENT

The present invention relates to security documents or tokens.

The term "security documents or tokens" used throughout the specification includes identity, value or entrance documents, which in turn respectively include: passports, visas, identity cards, drivers licences and security entrance cards; bank notes, shares, bonds, certificates, cheques, lottery tickets, bank cards, charge cards and credit cards; and aeroplane tickets, bus tickets, rail road tickets and tickets to fun parks or specific rides. These security documents or tokens typically include some form of authenticity verification to guard against copying and fraudulent alternation. The authenticity verification often includes a magnetic strip, but may include other forms of verification such as a signature and/or a photographic image.

In view of requirements for increasing levels of security, it is desirable to provide an alternative security document or token. It is also desirable to provide a security document or token which includes means for preventing or indicating fraudulent alteration.

In a first aspect of the present invention there is provided a security document or token comprising tamper evident means arranged for indication of an unauthentic security state of said security document or token upon exposure of said security document or token to one or more pre-determined conditions.

In a second aspect, the present invention provides a method of producing a security document or token comprising the steps of incorporating tamper-evident means for indication of an unauthentic security state of said security document or token upon exposure of said security document or token to one or more predetermined conditions.

The security document or token may comprise, for example, any one of the following: identity documents such as passports, visas, identity cards, drivers licenses, and security entrance cards; value documents such as bank notes,

shares, bonds, certificates, cheques, lottery tickets, bank cards, charge cards and credit cards; and entrance documents such as aeroplane tickets, bus tickets, railroad tickets and tickets to fun parks or specific rides.

Suitably, the security document or token includes security means for indicating an authentic security state of the security document or token. Preferably, the security means is arranged to indicate an authentic security state prior to exposure of the security document or token to the predetermined conditions.

In a preferred embodiment, the tamper evident means may be arranged, upon exposure of the security document or token to the predetermined conditions, to separate a portion of the security document or token from the remainder of the security document or token and prevent indication, by the security means, of the authentic security state. Preferably, the tamper evident means comprises a region which destructs or deforms upon exposure to the predetermined conditions to result in separation of said portion of said security document or token.

Alternatively or additionally, tamper evident means may be arranged to change appearance upon exposure to the predetermined conditions. For example, the tamper evident means may include a material which changes colour. The tamper evident means may operate independently of said security means, in which case the security means could indicate an authentic security state while the tamper evident means indicates an unauthentic security state when the security document is exposed to the predetermined conditions. However, the security means may be arranged to indicate an unauthentic security state upon exposure of said security document or token to the predetermined conditions.

The security means may comprise one or more security regions of the security document or token. In one preferred form of the present invention, the security means comprises two or more security regions so that an authentic security state is only indicated when said two or more security regions are authentically positioned relative to each other.

Preferably, said security means is arranged to indicate said security state visually. The security state is preferably determined by simultaneously viewing said two or more security regions.

Each security region may comprise a security layer or portion thereof. Preferably, two or more security layers are provided on opposite sides of a base layer with a tamper evident means provided between the base layer and at least one of the security layers. The security layer may comprise an opacifying layer. In one preferred form of the present invention, the security layer comprises a security coating, which may be a printed coating. Suitably, the printed coating is applied using one or more of the following printing processes: gravure, silk screen, off set and flexo.

The tamper evident means may comprise a tamper-evident separation region of the security document or token which is arranged to join said portion of said security document or token with said remainder of said security document or token when said security document or token is not exposed to said one or more predetermined conditions. The tamper-evident separation region is preferably predisposed to at least partially deform or destruct upon exposure to said one or more predetermined conditions. The separation region preferably comprises a tamper-evident layer of said security document.

In a preferred form of the invention, the tamper-evident region comprises a layer of a laminated security document or token. The tamper-evident layer may be a weakly coherent or adherent layer, e.g. formed of a material having a glass transition temperature which is lower than that of one or more other laminated layers of the security document or token.

The tamper-evident region may comprise an adhesive arranged to at least partly adhere two or more layers of a laminated security document. Alternatively, the document separation region may comprise a weakly coherent region of said security document resulting from coherence of laminated layers during formation of said security document. The weakly coherent region may be formed by application of heat and/or pressure.

The tamper-evident means may include a colour altering substance arranged to change colour responsive to said one or more predetermined conditions.

Suitably, the document separation means is arranged to separate said portion of said document from the remainder of said security document or token upon exposure of said security document or token to one or more predetermined conditions including, but not limited to, the following: a specific range of temperatures; a specific range of one or more forces; a specific range of impulses; and a specific range of pressures.

The invention will now be described, by way of example only, with reference to the accompanying drawing, in which:

Figure 1 is a schematic sectional view of an identity card in accordance with the invention.

Figure 1 shows an identity card 10, which is one form of security document or token referred to previously in the present specification. It will be readily apparent to a person skilled in the relevant art that the features of the identity card 10 and processes by which it can be produced apply to other security documents or tokens. It will also be readily apparent to a person skilled in the relevant art that specific forms of the identity card 10 include indicia (not shown) on either or both sides of the identity card 10.

The identity card 10 is formed of a number of layers, which are laminated to a support layer 12. The layers attached to one side of the support layer 12 can be identical to those attached to the other side of the support layer 12, in which case the identity card 10 is symmetrical about the support layer 12. However, different types of layers can be attached to each side of the support layer to form structurally different identity cards.

The support layer 12 is preferably formed from a substrate of a stable and robust polymeric material, such as polyethylene terepthlate (PET). A weakly

coherent or adherent tamper-evident layer 14, such as polyethylene (PE) is provided on the support layer 12, e.g. by extrusion. A security layer or coating 16 is applied to an outer surface of the tamper-evident layer 14 and an outer laminate or layer 18 of a stable and robust material, e.g. PET or polyvinyl chloride (PVC) is applied over the security coating 16. As explained above, the process can be repeated on the other side of the support layer 12 to form an identity card that is symmetrical about the support layer 12.

The security coating 16 and corresponding security coating 16' positioned on the other side of the support layer 12 are preferably arranged to form a composite design or image. The coatings may be formed of different forms of pigment coatings such as described in WO83/00659, the different forms containing different proportions of a major portion of pigment in a minor portion of polymeric binder. The security coatings may have different opacity levels to form the composite design and may be applied in a manner described in WO83/00659 which involves one or more of the following printing processes typically used in bank note printing: gravure; silk screen; offset; and flexo.

In an alternative form of the identity card 10, the security coatings 16, 16' may be formed from a single pigment coating. In this form of the identity card 10 different levels of opacity of the security coatings can be provided by varying the number of layers of regions of the security coatings.

The support layer 12 of PET has a high glass transition temperature, the tamper-evident PE layer 14 has a low glass transition temperature, the security coating 16 has a high glass transition temperature and the outer laminate layer 18 also has a high glass transition temperature. Preferably, the difference between the high and low glass transition temperatures is at least 30°C, and more preferably at least about 50°C. As will be readily apparent to persons skilled in the relevant field, layers 12, 14 and 18 can be formed of different materials to those listed above that have similar properties. For example, the support layer 12 may be formed of polycarbonate or polypropylene and the outer laminate layer 18 may be formed of polyvinyl chloride (PVC).

The outer laminate layer 18 may be attached to the security coating 16 using heat and pressure. An optional adhesive layer 20 may be used to enhance the bond between the security coating 16 and the outer laminate layer.

The identity card 10 can be personalised in a number of different ways. For example, prior to attachment of the outer laminate layer 18, printing 22 may be applied on the security coating 16 using, for example, offset printing, silk screen printing and/or ink jet printing. Alternatively or additionally, information can be attached to an outside surface of the outer laminate layer by dye-diffusion thermal transfer printing. Information can also be imprinted on outer and inner surfaces of the outer laminate layer 18 by intrusive techniques such as laser engraving.

The authenticity of the identity card 10 can be determined by simultaneously viewing the composite design formed by the security coating 16 and the corresponding security coating 16' positioned on the opposite side of the support layer 12. The security coatings are designed to be viewed by looking through at least partially clear laminated layers of the identity card 10 in a direction which is approximately perpendicular to planes in which the laminated layers lie, and are therefore positioned in a clear region of the identity card 10.

Fraudulent alteration of identity cards or other security documents or tokens can involve delamination of the security document. Delamination typically involves the application of heat until the temperature of the card is such that layers forming the card begin to delaminate. Once the security document has been delaminated variable data which is stored in the security document is accessible. Following alteration of the variable data, the security document is reassembled to conceal fraudulent alteration.

Attempts to delaminate the identity card 10 of the present invention using the application of heat either deform or destroy the low glass transition temperature PE layer 14 resulting in separation of the security coating 16 from the support layer 12 and from the security coating 16' on the other side of the support layer 12. Unless the security coating 16 is repositioned relative to the support layer 12 and corresponding security coating 16' using methods similar to those involved

in assembly of the authentic identity card 10, it is virtually impossible to reassemble the identity card 10 in an authentic manner.

One form of the identity card 10 is designed so that an authentic card requires the PE layer 14. In this form of the identity card 10, deformation, destruction or removal of the PE layer 14 affects visual interaction of the security coatings 16, 16' which are positioned on opposite sides of the support layer 12 to form the composite security design. Authentic visual interaction thus requires the presence of the tamper-evident PE layer 14.

Another form of the identity card 10 includes a tamper evident material (not shown) located in the tamper-evident layer 14. The tamper evident material may replace the security coating 16, or alternatively, provide an additional security feature. The tamper evident material can also be positioned on one or both sides of the support layer 12. The tamper evident material may be formed of a heat and/or oxygen sensitive material which changes colour upon the application of heat or exposure of the layer 14 to the atmosphere upon separation from the support layer 12. The change of colour of the tamper-evident layer 14 indicates that the identity card 10 has been tampered with and that it is not authentic.

It will be understood that the invention disclosed and defined in this specification extends to all alternative combinations of two or more of the individual features mentioned or evident from the text and/or drawings. All of these different combinations constitute various alternative aspects of the invention. Various changes and modifications may be made to the embodiments described and illustrated without departing from the present invention.

It will also be understood that the term "comprises" (or its grammatical variance) as used in this specification is equivalent to the term "includes" and should not be taken as excluding the presence of other elements or features.

Securency Pty Ltd

By their Registered Patent Attorneys
Freehills Carter Smith Beadle

14 November 2002

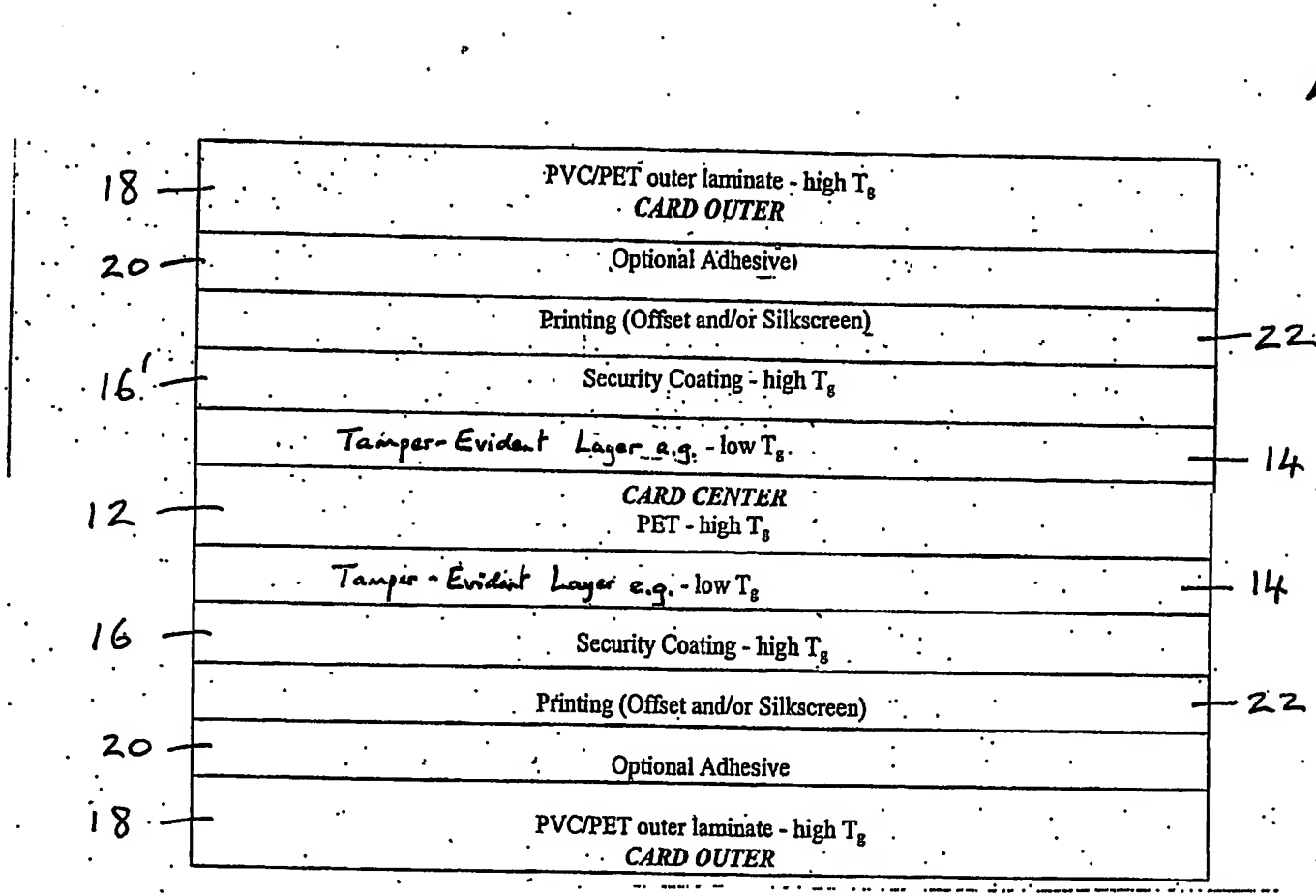

FIG. 1